Confidential! Please forward sealed!	**INVENTION DISCLOSURE** to Siemens AG or Subsidiary *Already faxed to CT IP* ☐ *Please be sure to indicate if applicable!*	CT IP file number *2002E17643 DE*
I/We (first name and surname of inventor(s) - further details and signature(s) on last page) Dr.Chris Winkler, Anton Schmitt, Johannes Bergmann	Number of inventors 3	Date of execution: 15.10.2002

report herewith the invention specified in full on the following pages with the title:

Method for coupling control components and network elements in IP networks

I. To superior/manager of inventor(s)

Received on:

Mr./Mrs./Ms. Prof. C Hoogendoorn ICN WN CS FP
(Department)

Please answer the following questions:

a) When did you receive the invention disclosure? → 22.10.2002

b) Is the invention based on publicly funded work?

☐ No ☒ Yes, project: KING (BMBF sponsored)

c) Is there a corresponding in-house R&D project?

☐ No ☒ Yes, project: KING (WN CS FP)

Legal term commences with date of receipt!

Only for CT inventions:

Project No. ____ Title: ____ Core technology: ____

☐ Development project In the interest of Group: ____ Contact: ____

☐ Research project

d) Filing is recommended ☐ No ☒ Yes

Urgency note

Costs borne by (organizational unit): ICN WN CS

☐ The invention does not lie in our field of interest. Following departments are to be consulted:

23.10.2002 C.H.Hoogendoorn

(Date) (Signature of superior/manager)

II. Please forward immediately on account of legal deadlines to

Siemens AG
CT IP (Patent Department)

Location: Mch P/Ri

for further action.

Received on:

CT IPS AM Mch P/Ri
Eing 24. Okt. 2002

1. Which technical problem is to be solved by your invention?
In future, alongside the internet and best-effort services common today, IP networks will also transport superior quality services and allow new applications. To this end, extensions to the network control facilities are required, for example in order to manage the network resources or to effect rapid reconfiguration in the event of a fault. For this purpose therefore in the KING project [1] for example the NAC (Network Admission Control) and NCS (Network Control Server) components are being introduced.

There are in general alternative means of integrating control components into the network components or of connecting them (directly or by way of a network connection) as separate servers to the network components (routers) to be controlled. The integrated solution has the advantage that as a result of the close coupling with the network component, internal information for this component is also available to the control facilities. By way of contrast, an "added" solution is manufacturer-independent and far more flexible because it is simply not so closely interwoven with the internal workings of the network component. Furthermore, "added" solutions can be based on standardized hardware/software solutions, whereas routers are mostly based on proprietary hardware/software solutions. This results in shorter development cycles and in cost savings.

By way of example of an Admission Control (AC) control component the problems associated with the server solution are to be discussed in the following and a method specified in point 3. as to how these problems can be solved.

The task of an Admission Control is to receive incoming resource requests, reconcile these with the resources remaining available and in the case of a positive assessment to program the router at the network edge (edge router network component) appropriately for controlling the data flow (setting functions such as marking, filtering, policing).

In this situation, the following two questions (*) arise, amongst others:

A) How do the resource requests reach the added AC?
B) How can the AC control/configure the edge router? In particular: From where does it obtain the necessary information concerning the internal workings of the router, which interface is to be configured for example.

In principle, two solution options exist for locating the AC component:

A) The data path taken by the IP packets is known and accordingly the AC component can be addressed directly (outband signaling).
B) The signaling protocol follows the path of the data packets and thus finds the AC component automatically (inband signaling).

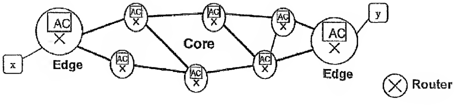
What follows is based exclusively on the signaling in accordance with variant B.

The standardized Resource Reservation Protocol RSVP [2] is an inband signaling protocol. It answers the questions (*) posed above, as described under 2. (see below). The key point here is that the RSVP entity is implemented in the edge router itself and can therefore operate very closely intermeshed with the router and its internal workings.

In this invention a method is specified which describes how separate control entities (taking an AC entity here by way of example) can be connected to a network component (an edge router here) and thereby answer the aforementioned questions.

2. How has this problem been solved up to now?
In addition, the example of an AC control component is considered in the following by way of example:

The standardized Resource Reservation Protocol RSVP [2] is implemented as part of the router and its control logic.



Taking an RSVP-enabled network having two connected subscribers X and Y by way of example (in other words a network having RSVP-enabled routers), the execution sequence will be described schematically as follows:
X generates a resource request to the network for its data stream to Y. In this situation it is necessary to ensure that the resource reservations in the routers are also actually made along the subsequent data path. In IP networks this data path depends on the current routing. Therefore, in RSVP, the resource request is sent into the network with the IP destination address of the subscriber Y and thus automatically follows the data path of the subsequent data stream to Y.
Although these messages are not actually addressed to them, the RSVP entities of the routers lying on the path must be made aware of them.
These messages are therefore specially identified by the well-defined IP protocol type "RSVP" in the IP header. The routers recognize this protocol type and pass on messages tagged in such a manner directly to their RSVP entity.

Later in the course of the procedure the RSVP entity must configure "its" edge router (filtering, marking, policing) at the network edge with X. In concrete terms, that interface is to be configured by way of which the RSVP message originally arrived from X and by way of which the data stream from X to Y will subsequently arrive. Since the RSVP entity is implemented in the router, it is able to interrogate this internal information.

The solution to both the aforementioned problems lies here in the close coupling between router and control entity:

A) The resource requests reach the AC entity by way of special filters in the router which recognize the protocol ID and pass the packets on directly to the AC entity, bypassing the routing.

B) The AC entity gains access to the information for configuration of the router by accessing router-internal databases.

3. How does your invention solve the specified technical problem (cite benefits)?
In this invention, a method is specified describing how the aforementioned problems can also be solved in the case of control entities implemented independently of the router, taking an AC entity here by way of example.

A.) How do the resource requests reach the AC?
The solution to this problem is obvious and is stated here primarily for the sake of completeness. Current routers support so-called policy routing whereby rules can be configured governing how to proceed with special packets. In this case the following rule applies:

> "Packets having a particular protocol ID are not simply routed onward (as a reminder: they are addressed to the subscriber Y) but are forwarded to a "next hop", preset as a general rule, which leads to the responsible external control entity."

Possible variants for connecting the control entity to the router are described under B).

B.) From where does the control entity obtain the internal information required for the configuration?
Here there is the problem that this information cannot be interrogated from the outside at the router (for example, the routing tables of the router only contain information about destinations, but not about where a packet came from).

The content of this invention is to include router-internal information which the control entity requires for configuration or other purposes with the data packet (in the example of the resource request) **to the control entity, in other words to suitably expand the packet with this information.**

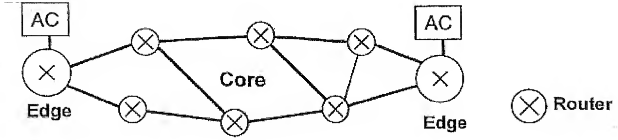
This can basically happen in two ways:

1. in a manner which can be executed using today's routers
2. with modification of the routers to support special tags/packet extensions

Solutions according to variant 1 are ideal for a rapid introduction into the networks.
For this purpose, several embodiment variants which can be executed using modern standard routers are proposed in the following.

1.) DSCP Marking

Prerequisite: Control entity is connected directly to an interface of the router, "added" to it in other words (cf. figure, AC here for example only at the edge routers).



This solution utilizes the policy function of modern routers.

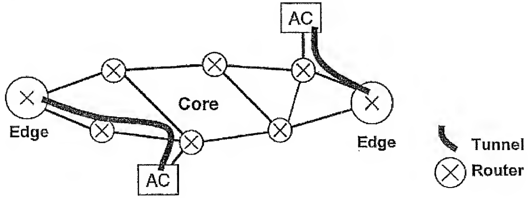
With regard to policy routing, in addition to a next hop it is also possible to specify in the rules which value the so-called DSCP field in the IP header (6 bits) should assume. In DiffServ networks [3] this serves to tag the packet priority. In the case of direct coupling of the control entity to the router by way of a separate interface, this DSCP information is however not required.

It is therefore possible to configure a rule on each input interface of the router which for example codes the number of the interface or other information into the DSCP field. It is thus possible to differentiate 64 values which can then be addressed by the control entity.

In the network itself, the DSCP value can nevertheless naturally be used in order to tag the packet priority because it can for example be set by the control entity to a different value. Furthermore, regardless of the "improper" use of the DSCP priority field, the packet can be processed with a selectable priority in the router in question itself because this can in general also be formulated in the router rule.

If more than 64 values are required, the DSCP field alone is not sufficient.

2.) Tunneling
A further way in which a standard router is able to tag packets are IP tunnels, GRE tunnels [4] for example. In the case of tunneling, the original IP packet is supplemented at the tunnel entry point by a tunnel header including a tunnel ID and a new, in other words external, IP header and is routed with this IP header through the IP network. At the tunnel exit point the external header is stripped off again and the original packet is processed further.



Modern routers, in particular the edge routers in question here, often support one or more tunneling variants.

The solution employing tunnels is based on the fact that a plurality of tunnels is set up from the router (start of tunnel) to the control entity (end point), which can be differentiated through their tunnel ID (in the tunnel header).

a) As one variant, the tunnel ID can now be used for the transfer of internal information, for example a separate tunnel per interface can be set up, such that the interface number corresponds explicitly or implicitly to the tunnel ID.

b) Equally, a combination of tunnels and additional use of DSCP marking (see 1.) is possible. For example, 2 tunnels and DSCP marking in order to differentiate 100 values, for example.

The rules on the interfaces then contain the corresponding tunnel and where applicable a DSCP marking as the "next hop".

With regard to the tunneling solution, the advantage furthermore arises that the control entity does not need to be connected directly to the router but can be placed anywhere in the network (cf. figure). It is then accessible by way of the logical "direct interface" "Tunnel". In this case, a DSCP marking according to 1. should be made on the inner IP header because then the DSCP of the outer header can actually be used for priority tagging.

3.) MPLS
Another form of tunneling is MPLS [5]. The method is similar to 2) except that instead of the IP tunnels MPLS "tunnels" or paths are used.

With the idea of adding router-internal information, for example interface no. or VPI/NCI numbers, to the control packets through suitable rules in the router it becomes possible to operate control entities independently of the router. The embodiment variants described can be implemented with today's routers. In this situation, the tunneling variants even allow the control entity to be set up anywhere in the network, in other words not necessarily directly at the router to be controlled.

This means that flexible and router-manufacturer-independent solutions for controlling network components can be produced. Moreover, these solutions are based on standardized hardware/software, whereas routers are for the most part based on proprietary hardware/software. This results in shorter development cycles and cost savings.

4. In what does the inventive step lie?
With this idea, control entities such as an Admission Control entity for example, can also be employed in today's IP networks without modification of the routers.
The inventive step lies in solving the basic problem by way of tagging the packets and also in the embodiment variants compatible with today's routers.

5. Exemplary embodiment[s] of the invention
Implementation within the scope of the KING project

References

No.	Author	Title etc.
[1]	K. Schrodi	Basis Erfindungsmeldung(en) zu KING [Basic invention disclosure(s) relating to KING]
[2]	IETF	RFC 2205 – RSVP
[3]	IETF	RFC 2474, RFC 2475 DiffServ
[4]	IETF	RFC 2784 GRE Tunneling
[5]	IETF	RFC 3031 MPLS

6. The following are enclosed for further explanation (in black and white where possible):

_____ sheet(s), representation of one or more exemplary embodiments of the invention;
(if possible, please enclose drawings in PowerPoint or Designer format)

_____ sheet(s), additional description (e.g. laboratory reports, test protocols);

_____ sheet(s), literature describing the prior art on which the invention is based; *)

_____ other documentation (e.g. floppy disks, particularly with drawings of the exemplary embodiments):

*) Please enclose photocopies or separate copies of all cited publications (papers complete; relevant chapter of books) with complete bibliographic data.

7. Which departments are interested in the invention? ICN WN
8. Has invention already been tested (tests performed, models constructed)?
   ☐ No ☒ Yes, result: Variant DSCP marking has been tested and works
9. For which products may the invention be used? Network components in IP networks, e.g. Next Generation Networks, SURPASS
10. Is the use of invention intended?
   ☐ No ☒ Yes, in: KING research project, KING demo, possible also field test
11. Has a product based on invention been delivered or is delivery intended?
   ☒ No ☐ Yes (probably) on ______ name of product: ______
12. Has the invention already been published or is the publication intended?
   ☒ No ☐ Yes, (probably) on ______ in book, journal: ______
13. Have third parties been informed of the invention or is such information intended?
   ☐ No ☒ Yes (probably) on 01.11.2002 to within the scope of the KING project
14. Please give as far as possible an assessment of the following criteria:

a Difficulty of circumvention for competitors
Alternatives of equal value
- ☐ Almost impossible
- ☒ Requires effort
- ☐ Easily possible

b Attractiveness of use for competitors
Interest by competitors
- ☐ Considerable
- ☐ Average
- ☐ Minimal

c Proof of use by competitors
Proof of use
- ☒ Easily possible
- ☐ Difficult
- ☐ Almost impossible

d Use within the company
- ☐ (probably) yes
- ☒ Open
- ☐ Unlikely